AMENDMENTS TO THE CLAIMS

Please cancel claims 1-5, 14-23 and 34-52 without prejudice or disclaimer.

1-5. (Canceled)

6. (Currently amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer;

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item and a document; and

replacing, by said third party, identification data of said candidate customer in said document with an identifier, and transmitting said document including said identifier to said business entity, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer as a transactional party in said electronic business transaction,

wherein a Fourth Party delivers to the customer a portable device P(C) which carries biometrics of the customer such that the customer can be identified as a legitimate owner of the portable device P(C) without revealing the identity of said customer,

wherein the device P(C) delivers a number S(C) at each transaction, and the number S(C) is readable from the portable device P(C) only in the presence of the customer,

~~The method according to claim 5,~~

wherein said portable device P(C) generates numbers S(C,n), where n is an integer belonging to a set {1, 2, . . . , N}, and

wherein for at least one of a new business entity and another partner of the customer, a new number n is chosen for all further transactions between the customer and said at least one of said new business unit and said another partner.

7. (Currently amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer;

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item and a document; and

replacing, by said third party, identification data of said candidate customer in said document with an identifier, and transmitting said document including said identifier to said business entity, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer as a transactional party in said electronic business transaction,

~~The method according to claim 2,~~

wherein the business entity chooses a set of verifiers Vj, j = 1, 2, . . .N, and

wherein said verifiers are each equipped to verify portable devices, and are connectable to a network so as to output information to a third party T using privacy protection.

8. (Currently amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer;

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item and a document; and

replacing, by said third party, identification data of said candidate customer in said document with an identifier, and transmitting said document including said identifier to said business entity, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer as a transactional party in said electronic business transaction.

~~The method according to claim 2,~~

wherein said establishing an intermediary relationship includes sending by the customer to the third party said document to register with said business entity and software to encrypt the document using a public key pu1(I) included in a public signature scheme (Pr1(I),pu1(I)) of the business entity, said software further allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), and said document being provided over a network connected to said business entity.

9. (Previously presented) The method according to claim 8, wherein the document comprises a header having identification data about the customer written together with a number S(C) associated with the proprietary item, and a body where personal or other data associated with said customer and pu2(I,C) are written after encryption using pu1(I).

10. (Previously presented) The method according to claim 9, wherein when receiving the document, the third party replaces the header with a number N(T,C,I) which is sent to insurance entity with body of the completed document, wherein said business entity decrypts body and decides on an offer price if any, and

wherein a decision is communicated to the business entity after encryption using pu2(I,C) together with N(T,C,I), and the business entity forwards pu2(I,C)(D) to the customer.

11. (Currently amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer;

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item and a document; and

replacing, by said third party, identification data of said candidate customer in said document with an identifier, and transmitting said document including said identifier to said business entity, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer as a transactional party in said electronic business transaction,

~~The method according to claim 2,~~

wherein, before establishing an intermediary relationship, the customer accesses one or more verifiers Vj, and

wherein the customer identifies itself to each verifier Vj using a number S(C) associated with the proprietary item, and requests Vj to send S(C) to the business entity, together with data verified by Vj.

12. (Previously presented) The method according to claim 11, wherein communication to the business entity is performed by appending to the number S(C) a non-identity data relevant to the customer encrypted using pu1(I).

13. (Previously presented) The method according to claim 11, wherein a link between the third party and the business entity is provided by the third party posting one or more completed documents on a dedicated world-wide-web (WWW) page after replacing said identification data with said identifier, and

wherein said identifier comprises a number N(T,C, I) which allows the business entity, but no other party, to recognize this number as a number associated with the business entity.

14-23. (Canceled)

24. (Previously presented) A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

sending, by a customer to a third party, an application and software for encrypting the application using a public key pu1(I),

wherein said application is taken electronically from a business entity,

wherein a public signature scheme of said business entity is (Pr1(I),pu1(I)), software allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), and

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction,

wherein said third party replaces identification data of said customer with an identifier in said application which is transmitted to said business entity,

wherein said method further comprises:

establishing a customer-purveyor contact over the network, said establishing comprising

when submitting a transaction request, encrypted using pi1(I), the customer addresses the request to the third party, after selectively accessing one or more verifiers Vj;

transmitting, by the third party T, the transaction request to the business entity after removing a header and attaching a number Ntransaction(T,C,I,Transaction) thereto;

processing the request by the business entity;

sending, by the business entity, a communication to the third party;

transmitting said communication, after or while processing the transaction request, to the third party, said request being encrypted using the public key pu2(I,C); and

transmitting, by the third party, the communication to the customer.

25. (Previously presented) The method according to claim 24, wherein the application includes a header where said identification data is written together with a number S(C), and a body where other data of the customer and the key pu2(I,C) is written after encryption using the public key pu1(I).

26. (Previously presented) The method according to claim 25, wherein when receiving the application, the third party replaces the header with said identifier which comprises a number N(T,C,I) which is sent to the business entity with the completed body of the application.

27. (Original) The method according to claim 26, wherein the business entity decrypts the body using Pr1(I)(pu1(DATA)) and makes a decision D on whether to proceed and if so, an offer price, and

wherein the decision D is communicated to the third party after encryption using public key pu2(I,C) together with the number N(T,C,I), and

wherein the third party, using the number N(T,C,I) to recognize the customer, sends the public key pu2(I,C)(D) to the customer, who decrypts using a private key Pr2(I,C) to obtain D = Pr2(I,C)(pu2(I,C)(D)).

28. (Previously presented) The method according to claim 24, wherein before sending said application to the business entity, the customer accesses one or more verifiers.

29 - 32. (Canceled)

33. (Previously presented) The method according to claim 24, wherein the communication includes one of a payment, a request for further data, and a declination of part or all of the transaction.

34-52. (Canceled)